Information Assurance (IA) and the DoD Acquisition Process

Information Briefing *for* *DAU – Alumni Association Symposium* *17-18 June 2003*

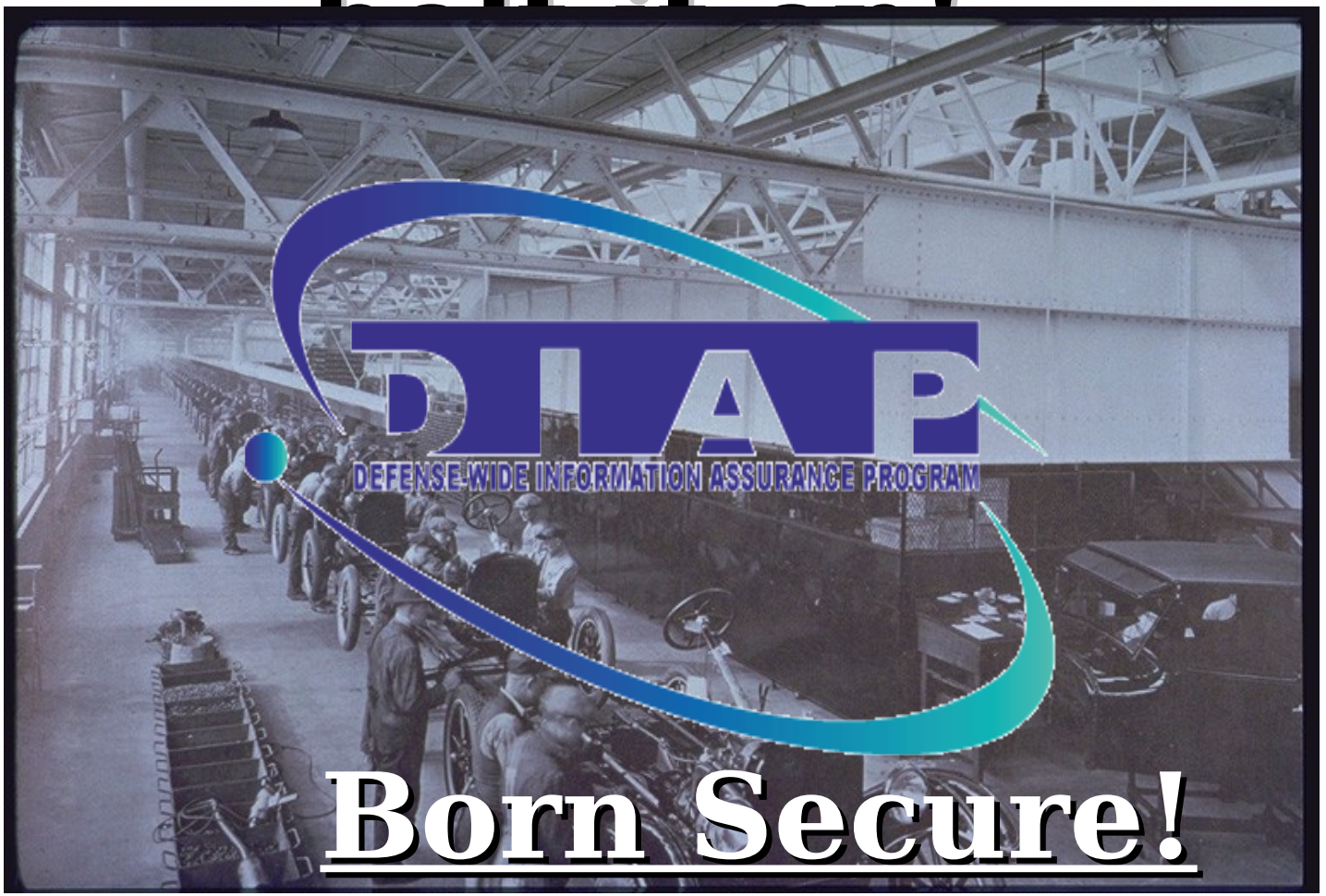
Mr. Eustace King
Technology & Capabilities, Group Lead
Defense-Wide Information Assurance Program (DIAP)
eustace.king@osd.mil
(703) 602-9969

AGENDA TOPICS

- Guidance from Top Management
- Threats
- Regulations
- DIAP Roles/Responsibilities
- IA Strategy
- Current Initiatives
- Q&A

in…

Don’t


DIAP
DEFENSE-WIDE INFORMATION ASSURANCE PROGRAM
Born Secure!

Information Assurance – Emphasis Starts at the Top

SECDEF's Transformational Goals*:

- First, to defend the U.S. homeland and other bases of operations, and defeat nuclear, biological and chemical weapons and their means of delivery;
- Second, to deny enemies sanctuary—depriving them of the ability to run or hide—anytime, anywhere.
- Third, to project and sustain forces in distant theaters in the face of access denial threats;
- Fourth, to conduct effective operations in space;
- **Fifth, to conduct effective information operations; and,**
- **Sixth, to leverage information technology to give our joint forces a common operational picture.**

"….<u>Protect</u> our information networks from attack"…

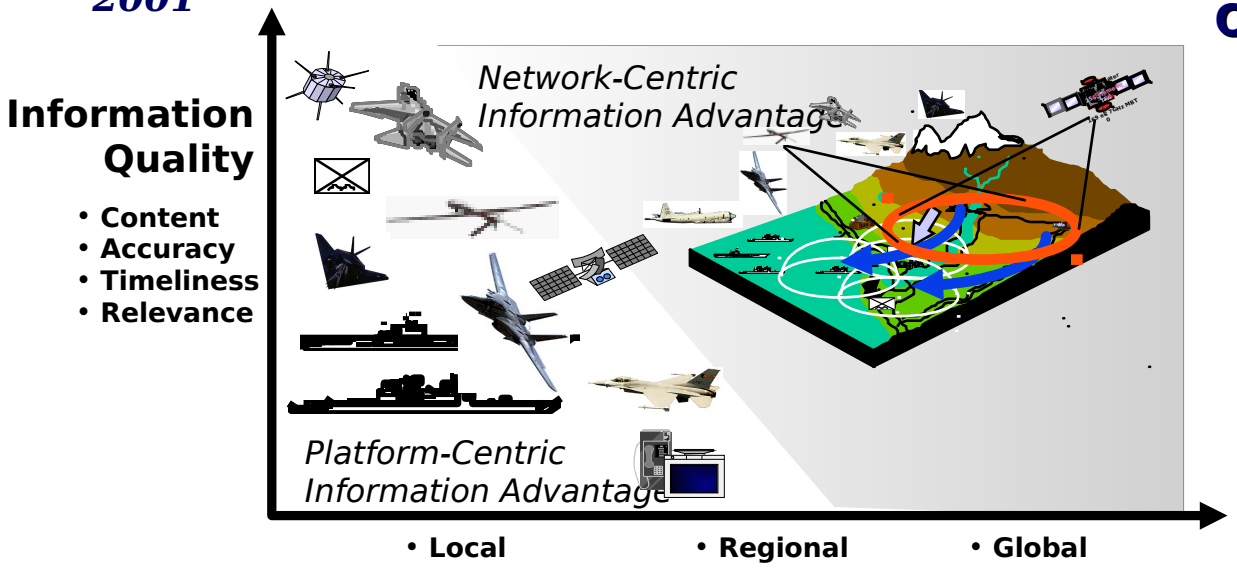
…Use information technology to link up different kinds of US forces so that they can in

* From Secretary Rumfeld's speech to the National Defense University 21 Jan 2002

Transformation

"The ***two truly transforming things***, conceivably, might be in information technology and information operation and ***networking and connecting things in ways that they function totally differently than they had previously***. And if that's possible, what I just said, that possibly the ***single-most transforming thing*** in our force will not be a weapon system, but ***a set of interconnections*** and a substantially enhanced capability because of that awareness."

Secretary Rumsfeld, Aug 9, 2001

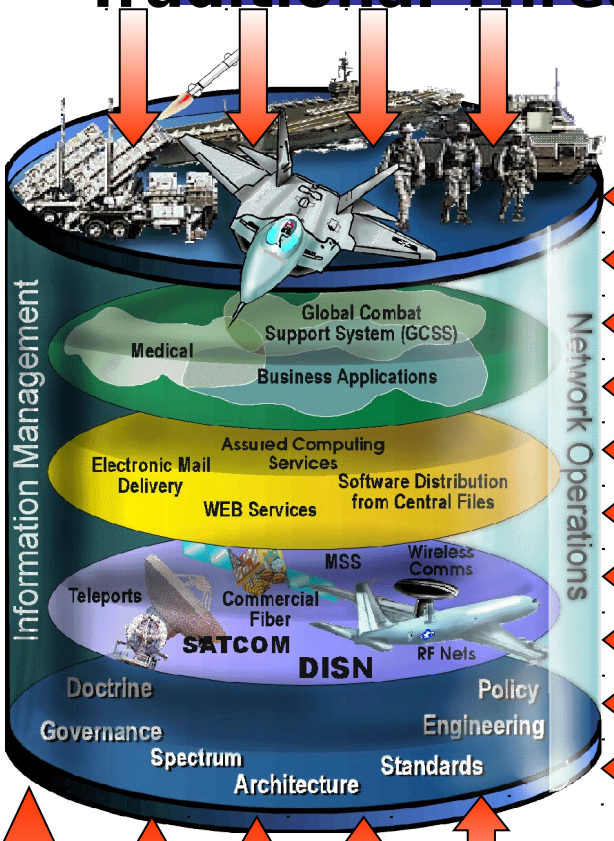


Network-Centric Operations:

- **Military operations** enabled by "Networking the Force"
- "Networking the Force" is accomplished through **distributed collaboration processes** designed to ensure that **all pertinent available information is shared** and that all appropriate assets can be brought to bear to by commanders **to employ dominant maneuver, precision engagement, full-dimensional protection, and focused logistics**.

Threats to the Global Information Grid

Traditional Threats



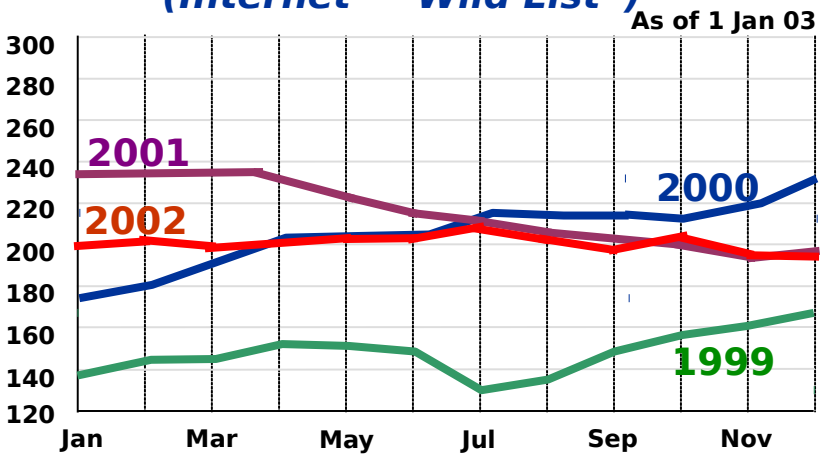
Non-Traditional & Emerging Threats

- Computer Network Operations
- Cleared "Insiders"
- Viruses
- Electro Magnetic Pulse Attack
- Crypto Attacks
- Nodal Attacks on Networks
- Terrorism vs. Critical Infrastructure
- Attacks on Critical Infrastructure
- Commercial Pressure on Spectrum
- Competing Demands on Resources

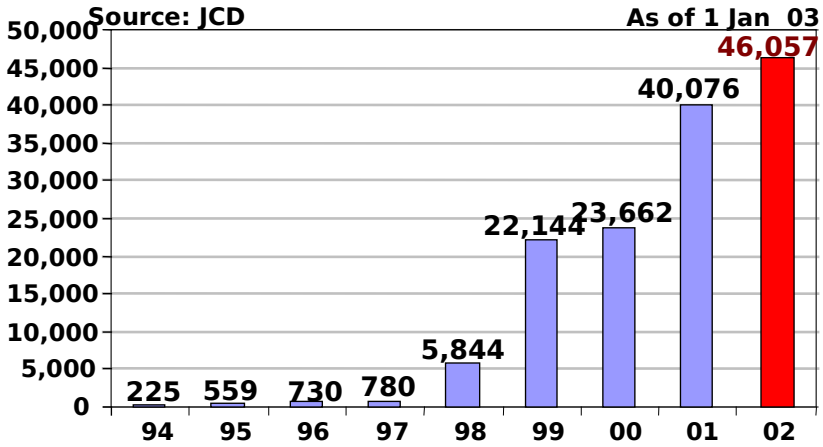
- Outmoded Protection Policies
- Unqualified Workforce
- Law Enforcement vs. National Security Focus
- Slow Government Cycle Times
- Globalization

Malicious Activity Continues to Climb

Virus Growth Per Month
(Internet - "Wild List")



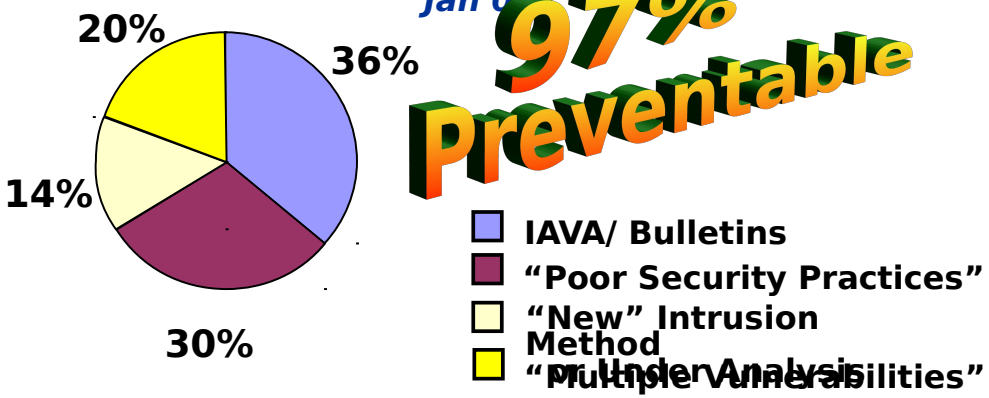
Detected "Events"
(DoD Unclassified Network "NIPRNet")



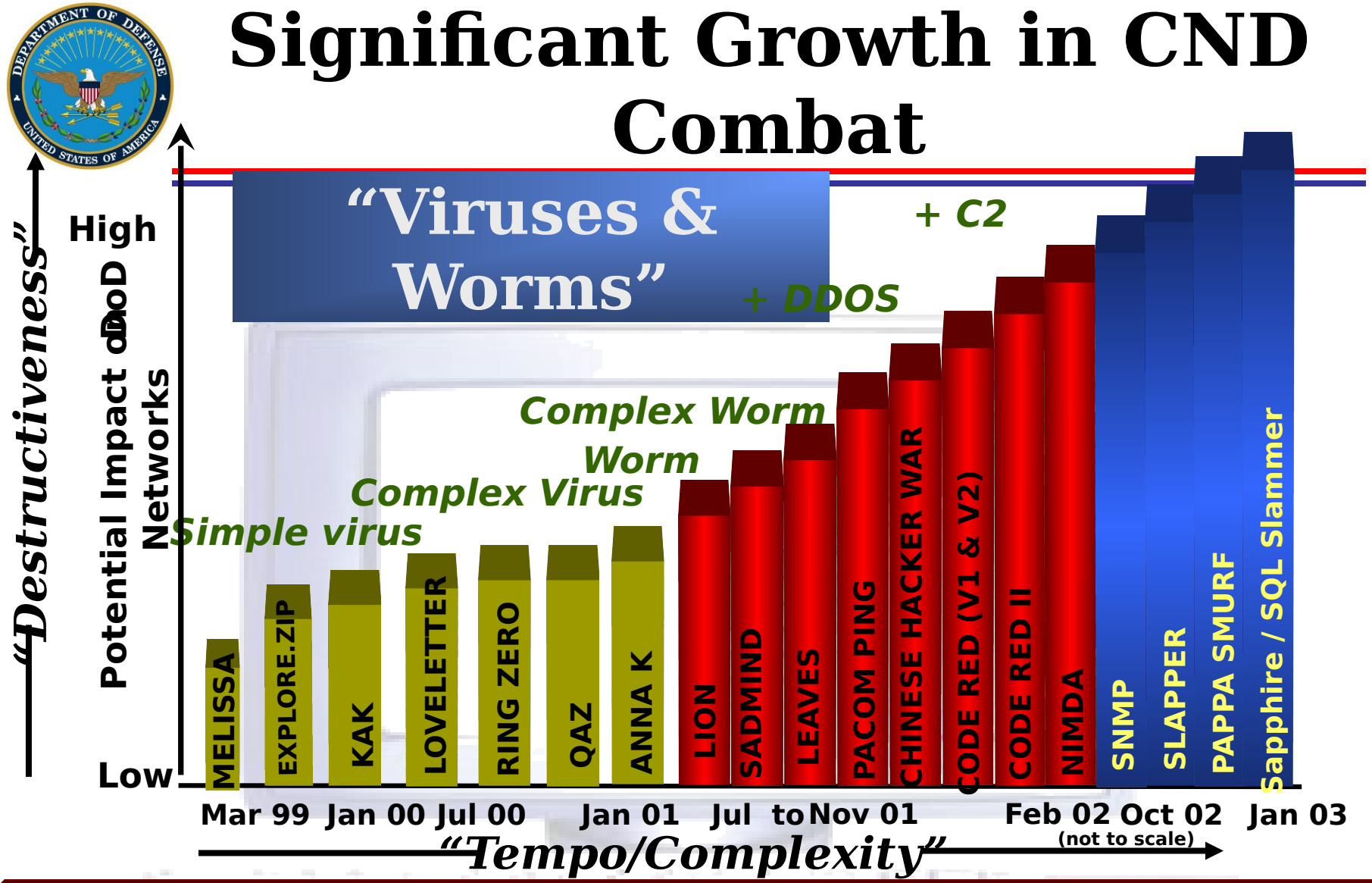
"Information Networks must be controlled, protected, and managed as effectively as weapon systems"

Lt Gen Harry D. Raduege, DISA Director

Unauthorized DoD Intrusions
(314 Category 1 & 2 Intrusions as of 1 Jan 03)



Significant Growth in CND Combat



Tempo, Complexity, Destructiveness – All Increasing!

The Challenge

- Growing dependence on information systems
- Rapid growth in computer networks
- Vulnerability to internal and external attack

NIPRNET Growth

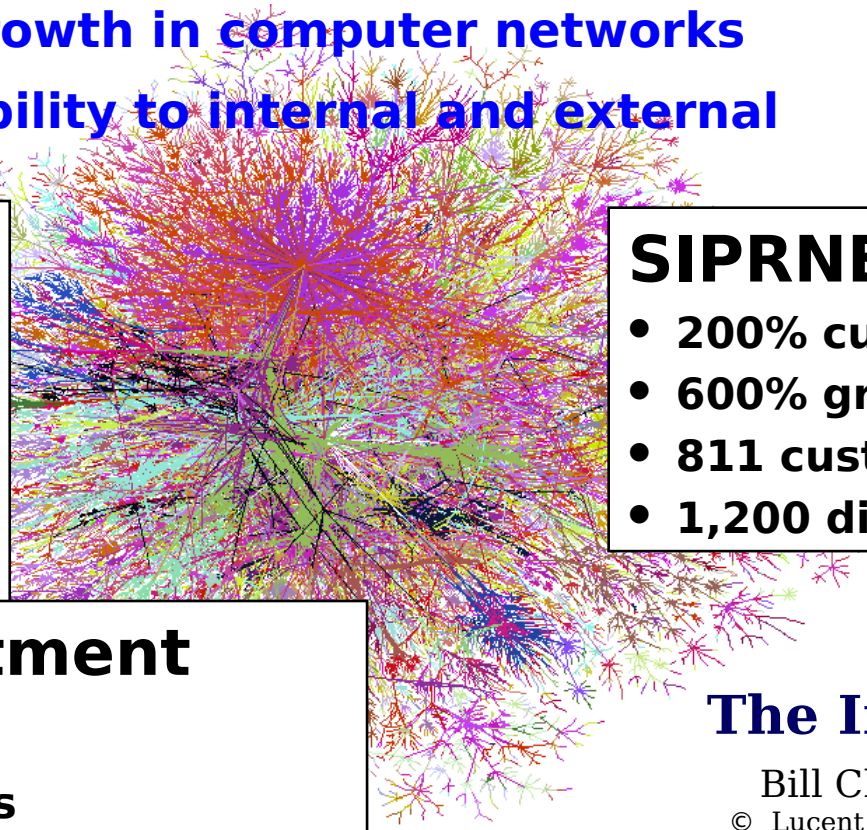
- 20% customer growth*
- 400% growth in traffic*

SIPRNET Growth

- 200% customer growth*
- 600% growth in traffic*
- 811 customers
- 1,200 dial-up users

Defense Department Systems

- 2-3 Million Computers
- 100,000 Local Area Networks
- 100 Long-distance Networks



The Internet

Bill Cheswick

Key Acquisition Regulations for IA

- AT&L
  - DoD Directive 5000.1, The Defense Acquisition System; Signed 12 May 2003
  - DoD Instruction 5000.2, Operation of the Defense Acquisition System; Signed 12 May 2003
  - DoD Regulation 5000.2-R, Discretionary Guidebook
- USG
  - Clinger-Cohen Act of 1996
  - NSTISSP-11, National IA Acquisition Policy
- C3I
  - DoD Directive 8500.1, Information Assurance
  - DoD Instruction 8500.2, Information Assurance Implementation
  - DoD IA Strategy
  - DoD Instruction 8580.aa, IA Acquisition

IA in DoD Directive 5000.1

- **3.10 – Information Assurance.**
  - Information Assurance requirements **shall be addressed** for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems; and information technology programs that are dependent on external information sources, or that provide information to other DoD systems.

IA in DoD Instruction 5000.2

- **E4.1.1. Mission-Critical Information System.** A system that meets the definitions of "information system" and "national security system" in the CCA, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: The designation of mission critical should be made by a Component Head, a Combatant Commander, or their designee.) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."
- **E4.1.2. Mission-Essential Information System.** A system that meets the definition of "information system", that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: The designation of mission essential should be made by a Component Head, a Combatant Commander, or their designee.) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."

IA in DoD Regulation 5000.2-R

- **C6.6.1.** PMs shall manage and engineer information systems using the best processes and practices known to reduce security risks, including the risks to timely accreditation. Per DoD Instruction 5200.40, they shall address information assurance requirements throughout the life cycle of all DoD systems. The PM shall incorporate approved CRD-derived and ORD-derived information assurance requirements into program design activities to ensure appropriate availability, integrity, authentication, confidentiality, and non-repudiation of program and system information and the information systems themselves, as specified in the applicable SSAA. PMs shall also provide for the survivability of information by incorporating protection, detection, reaction, and reconstitution capabilities into the system design, as appropriate, and as allocated in SSAAs.

This regulation has become discretionary guidance

Clinger-Cohen Act of 1996

- **DoD 5000.2, Enclosure 4, Table 1**
  - **Requirements related to CCA:**
  - "The program has an Information Assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards".
- **Applicable Program Documentation:**
  - An Information Assurance Strategy

NSTISSP-11 National IA Acquisition Policy

- Effective 1 Jan 2001: Preference given to acquisition of evaluated COTS Information Assurance (IA) and IA-enabled products

- Effective 1 Jul 2002:
  - Acquisition of ALL COTS IA and IA-enabled products limited to those on NIAP Validated Products List or NIST Crypto Module Validation List
  - Acquisition of GOTS IA and IA-enabled products limited to NSA approved
  - Waivers reviewed by NSA and granted on case-by- case basis by CNSS

DoD Directive 8500.1 Information Assurance

- New Policy Numbering Series for IA – “8500”
- New Definitions – A “Must Read”
  - DoD Information Systems:
    AIS Applications Outsourced IT-based Processes
    Enclaves Platform IT Interconnections
  - Sensitive Information
  - Community Risk
  - Need-to-Know
  - IAM/IAO
  - DMZ
- Acquisition Policy (NSTISSP 11)
- Focus on Enterprise and Interconnections
- Baseline Sets of Graded IA Controls – (Banded Risk)
- Mission Assurance Categories
- IA as a component of Mission Readiness (JQRR)

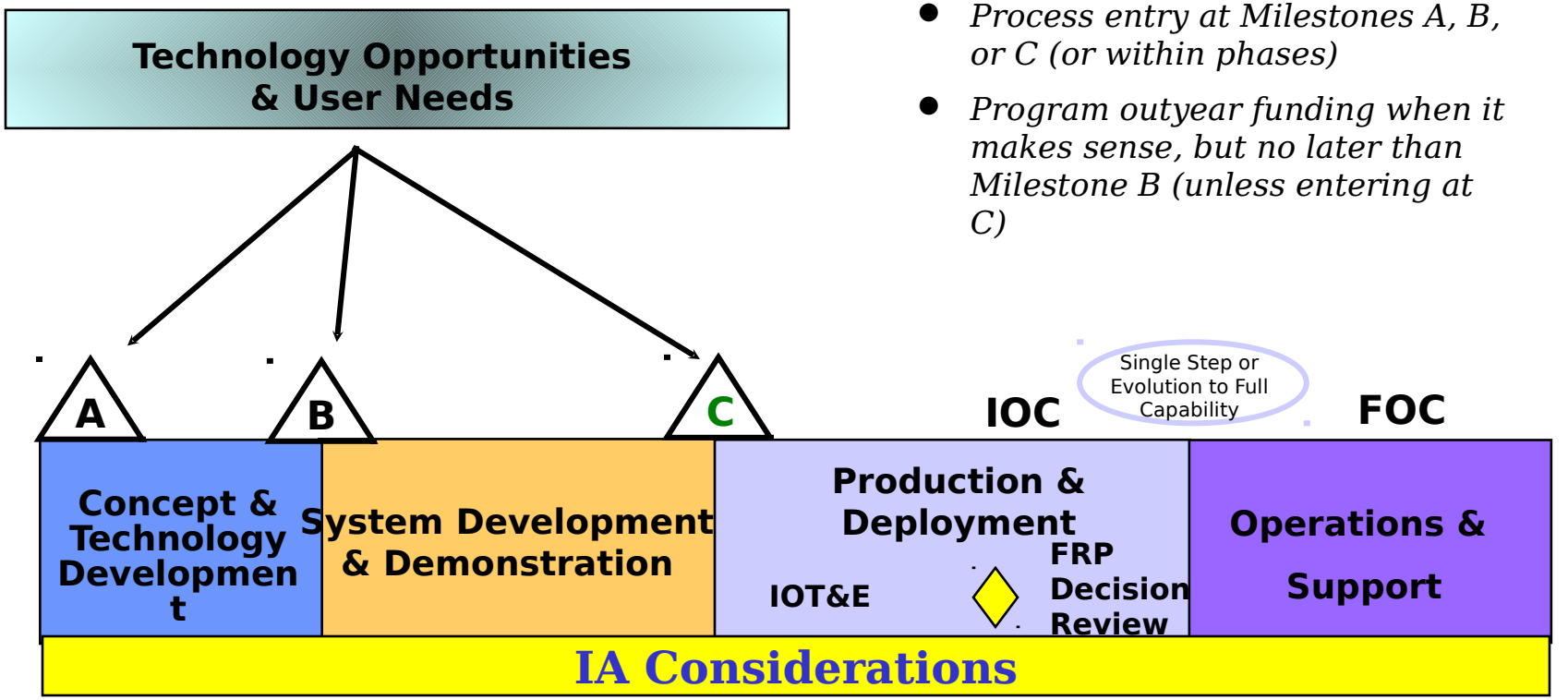
DoD Instruction 8500.2 IA Implementation

Determines Baseline IA Controls for Availability & Integrity:

- **Mission Assurance Category I:**
  - Vital to Mission Effectiveness or Operational Readiness of Deployed or Contingency Forces
  - Loss or Degradation Results in Immediate and Sustained Loss of Mission Effectiveness
  - Must be Highly Accurate and Highly Available
  - Most Stringent Protection Measures Required
- **Mission Assurance Category II:**
  - Important to Support of Deployed or Contingency Forces
  - Loss or Degradation Could Delay Services or Commodities Essential for Operational Readiness or Mission Effectiveness
  - Loss of Integrity is Unacceptable
  - Loss of Availability Difficult to Manage; only tolerable for short term
  - Additional Safeguards Beyond Best Practices Required
- **Mission Assurance Category III:**
  - Needed for Day-to-Day Business, Does Not Affect Support to Deployed or Contingency Forces in the short-term
  - Loss Can Be Tolerated or Overcome without Significant Impact on Mission Effectiveness or Operational Readiness – Can be Reconstituted
  - Protective Measures Commensurate with Commercial Best Practices

The DOD 5000 Model
IA is MORE than DITSCAP

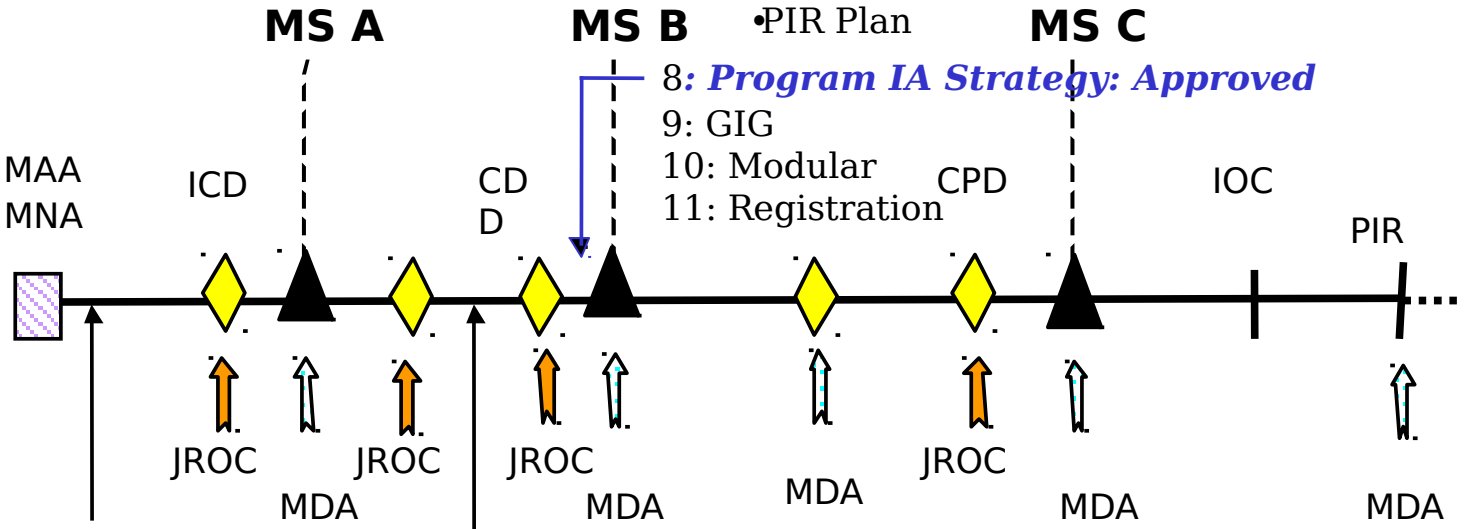
- *Process entry at Milestones A, B, or C (or within phases)*
- *Program outyear funding when it makes sense, but no later than Milestone B (unless entering at C)*



Integrating CCA in Acquisition Phases & Milestones

(and where IA fits into the puzzle)

	Determination of Mission Need	*Concept & Technology Development*	*System Development & Demonstration*	*Production & Deployment*
EXIT CRITERIA	•IPT Structure •**AS** •**APB** •Threat Assess	•Update BPR, AS •**TEMP**, PM Plan, SEMP •**C4ISP**, ***SSAA***, Interop Cert •CARD, CCA, Log Strategy •Risk Mgmt Plan, SAMP	•Update SAMP •IV&V •IOT&E •Roll-out Plan •ILSP •PIR Plan	•Maintenance •FOT&E •PIR Analysis



1: Core Function Need to be Performed by GIG
2: No Private or Gov Source can Better Support function
3: BPR

With IA Inputs

4: AoA
5: EA
6: Acquisition Measures
7: Mission Performance Measures

DODI 5000.2
CCA Requirements
Enclosure 4, Table 1

AUTHORITY FOR EXISTENCE OF DIAP

- **DEPSECDEF Memo 30 Jan 1998**
- **DOD CIO Memo 12 Feb 1999**
- **Sec 1043 National Defense Authorization Act for FY 2000**
  - **“(a) IN GENERAL - Chapter 131 of title 10, United States Code, is amended by adding at the end the following new section:**
  - **Section 2224. Defense Information Assurance Program**
  - **(a) DEFENSE INFORMATION ASSURANCE PROGRAM - The Secretary of Defense shall carry out a program, to be known as the Defense Information Assurance Program, to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crises…”**

DIAP Director

- Chief of Staff
- Admin Assistant
- Deputy Director
  - Resource Management Team
  - Operations
    - Readiness
    - Net Ops
    - AS&W
    - Assessments
    - Connection, Approval, Recert
    - Policy
    - Joint Staff Liaison
    - Law Enforcement & CI Coordinator
    - Critical Infrastructure
    - Reserve Component Liaison
    - Agency Liaison
    - Service Liaison
    - I/C Coordinator
  - Human Resources
    - Education
    - IA Scholarships
    - Training
    - Awareness Activities
    - Website Support
    - Personnel & Manpower
  - Technology Deployment
    - Research & Technology
    - Acquisition Pro… Su…
    - Ar…
    - Requirements

Acquisition & Product Support

Eustace King 703-602-9969

Rick Harvey 703-845-6670

Frank Curtis 703-602-9995

Arthur King 703-604-1480 ext 104

Eric Jan 703-604-1480

Wil… 9974

EM… Fi… @osd.

DIAP Roles/Responsibilities

- Oversight
  - Policy
  - MDAPS/MAIS
  - CND Assessments
  - IA Education, Training, and Awareness
- Resource Priorities/Deconfliction
  - S&T
  - Initiatives
  - Programs
  - C/S/A POMS
  - Execution Oversight
- Reporting/Assessing/Evaluating
  - FISMA/GISRA
  - GAO
  - DoD IG
  - DoD IA Annual Report (Congress)

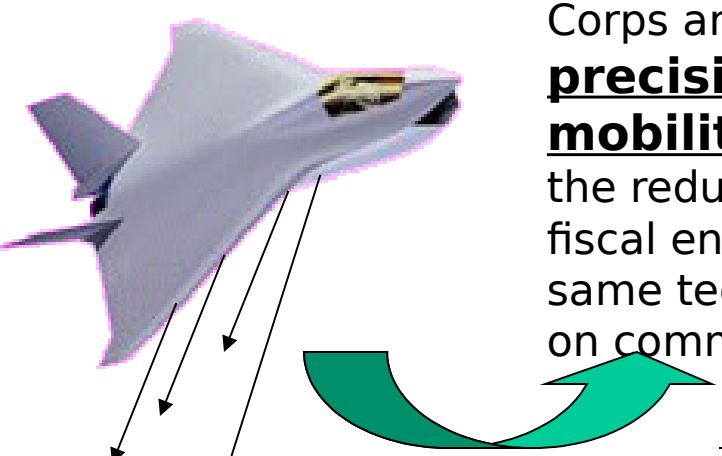
Think IA is Not Your Problem??

"…but I'm a weapon system, not an information system!"

However…

…

The Joint Strike Fighter (JSF) is a multi-role fighter optimized for the air-to-ground role, designed to affordably meet the needs of the Air Force, Navy, Marine Corps and allies, with **improved survivability, precision engagement capability, the mobility necessary** for future joint operations and the reduced life cycle costs associated with tomorrow's fiscal environment. JSF will benefit from many of the same technologies developed for F-22 and will capitalize on commonality and modularity to maximize affordability.



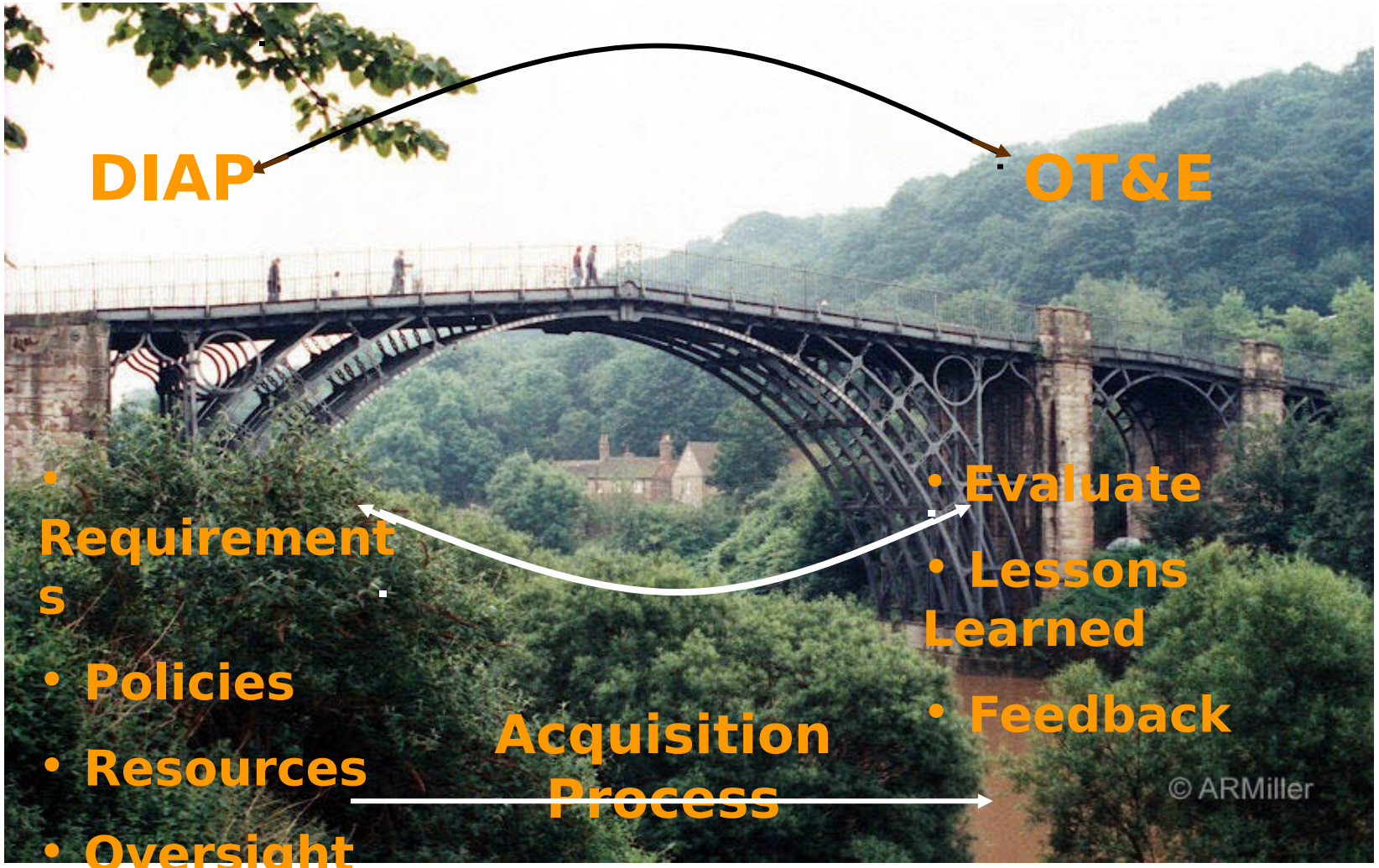
….if you don't protect the links, you

Global Information Grid

DAU 17-18 I

Won't fulfill the mission….

DIAP/OT&E Feedback Loop



DOD's INFORMATION ASSURANCE STRATEGIC PLAN FRAMEWORK

VISION

Achieve Dynamic Information Assurance in support of Mission Dominance

MISSION

Assure DoD's Information, Information Systems, and Information Infrastructure

GOALS / OBJECTIVES

Protect Information to ensure that all information has a level of trust commensurate with mission needs by…

- Defining data protection requirements for Network-Centric Operations
- Applying protection mechanisms across the enterprise
- Developing robust mechanisms that protect information

Defend Systems and Networks to ensure that no access is uncontrolled and that all systems and networks are capable of self defense by…

- Engineering system and network defenses
- Reacting to events and responding to threats and deficiencies
- Assessing and evaluating systems and network activity

Provide Integrated IA Situational Awareness / IA Command and Control (C2) to provide a shared understanding among decision makers and the decision tools necessary for coordinated actions by…

- Creating an integrated Operational Picture with near-real-time information sharing and understanding with insight into military operations
- Coordinating IA operations and decision making
- Evaluating collaboration across the extended enterprise

Improve and Integrate IA Transformation Processes to develop and deliver dynamic IA capabilities and to improve inter- and intra-entity coordination and improve risk-reduction and return on investment by…

- Ensuring IA is integrated into all DoD programs
- Integrating and improving the development and delivery of dynamic IA capabilities
- Improving the quality of strategic decision-making
- Improving information sharing with others

Create an IA-Empowered Workforce that is trained, highly skilled, knowledgeable, and aware of its role in assuring information by…

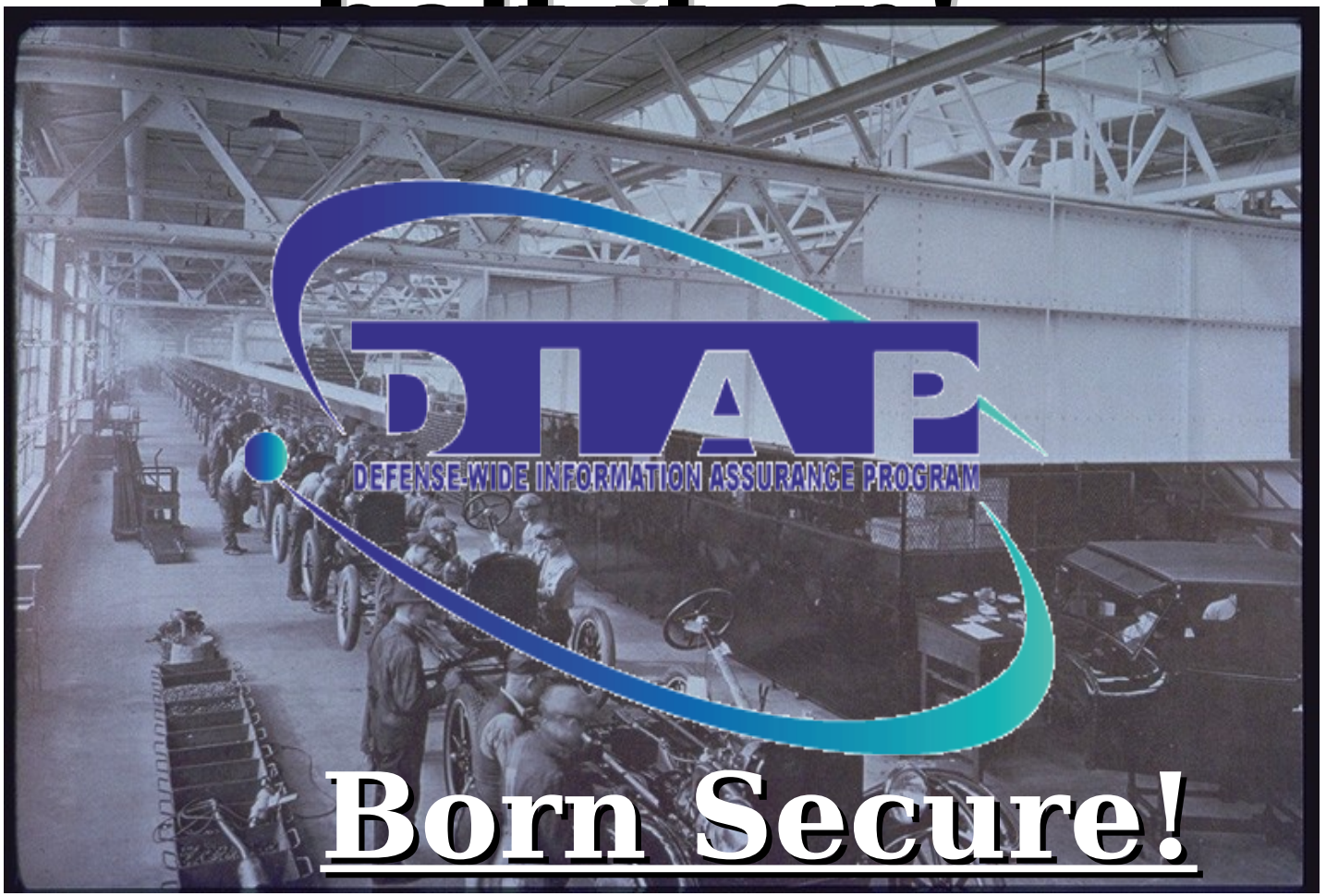
- Standardizing baseline IA skills across the enterprise
- Continuously enhancing IA skill levels
- Providing trained / skilled personnel when and where needed
- Infusing IA into other disciplines

Initiatives to Improve IA (throughout the Acquisition Life Cycle)

- Publish IA Strategy
- Promulgate IA acquisition strategy guidance (DoD 8580.1)
- Net-Ready KPP – combines Interoperability, IA, & Data Quality
- Software Assurance Initiative
- Ports and Protocols
- IA Testing of Fielded Systems

in…

Don’t


DIAP
DEFENSE-WIDE INFORMATION ASSURANCE PROGRAM
Born Secure!

DIAP Points of Contact & Important Websites

- COL Gene Tyler 703/602-9988 gene.tyler@osd.mil
- Robert Gorrie 703/602-5042 gorrie.robert@osd.mil
- Eustace King 703/602-9969 eustace.king@osd.mil
- Rick Harvey 703/845-6670 rharvey@ida.org
- Eric Jan 703/604-1480 eric.jan@osd.mil
- Arthur King 703/604-1480 arthur.king@osd.mil

- www.iase.disa.mil (DISA)
- www.nstissc.gov (NSTISSP-11)
- www.c3i.osd.mil (C3I)
- www.c3i.osd.mil/org/sio/ia/diap (DIAP)

I WANT YOU
for INFORMATION
ASSURANCE

ACQUISITION